"Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State Sponsored Cyber Actors"

Testimony before
House Natural Resources Committee,
Subcommittee on Oversight and Investigations

June 7, 2023

Dean Cheng

Senior Advisor

United States Institute of Peace

My name is Dean Cheng. I am a non-resident Senior Fellow at the Potomac Institute for Policy Studies, and a Senior Adviser with the United States Institute of peace. The views I express in this testimony are my own, and should not be construed as representing any official position of either the Potomac Institute or the United States Institute of Peace.

Chinese View of Information

Over the past half century, the leadership of the People's Republic of China (PRC) has increasingly emphasized the importance of information as it relates to national economic development and national security. Beginning in the 1970s, the proliferation of microelectronics, computers, and telecommunications technology has accelerated the ability to gather, store, manage, and transmit information. From the perspective of the Chinese Communist Party (CCP) leadership, information technology, including computers and telecommunications systems, have permeated all aspects of society and economies and become an integral part of a nation's infrastructure.[1] Chinese analysts have dubbed this process "informationization (*xinxihua*; 信息化)," and see the world as shifting from the Industrial Age to the Information Age.

From the Chinese perspective,

> Informationization is a comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the

[1] TAN Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," ***National Defense Science and Technology*** (#5, 2009), p. 72.

> support, where information talent is a key factor, where laws, policies, and standards are the safeguard.[2]

In the face of this broad trend of economic, political, and social informationization, Chinese analysts have concluded that national economic development requires greater integration of information technologies into all aspects of the economy, while defending against threats to PRC national interests and security also must become informationized.

Economic development in the Information Age is built upon accessing, exploiting as well as analyzing and transmitting information. While manufacturing, transportation, and other traditional industries remain an essential part of a nation's strength, even those are increasingly digitized, whether in terms of the designs that they are producing or the electronic controls that govern the manufacturing equipment and power networks that sustain them. Information technology therefore permeates all aspects of the nation's economy, indirectly as well as directly.

The spread of information technology similarly means that potential adversaries have unprecedented access to each others' national economy, as well as the broader population and the top decision-makers. Just as the bomber and ICBM allows an opponent to directly strike a nation without having to first break through ground or naval defenses, information technology similarly outflanks traditional military forces. The proliferation of information technology into society and economics makes a nation broadly vulnerable to a range of new pressures and threats.

These threats extend beyond information networks (e.g., vulnerability to denial-of-service attacks) and component computers (e.g., computer viruses, malware). Instead, the very information itself can constitute a threat, if, for example, its content erodes the morale of key decision-makers, popular support for a conflict, or the will of the military to fight. Consequently, China's interpretation of its national interests has expanded, in step with the expanding impact of information writ large on China.

More recent advances in information technology, including artificial intelligence and machine learning, the Internet of Things (IoT), big data and cloud computing, have further underscored the

[2] State Council Information Office, Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans (October 18, 2002), http://www.cia.org.cn/information/information_01_xxhgh_3.htm

growing reach and capability of those able to exploit information networks through network warfare and cyber operations. These advances also affect both economic and security calculations.

PRC Employment of Network and Cyber Operations

Because of the growth of interconnectivity, the CCP is able to exploit its network and cyber capabilities for both economic and national security gains.

In the military and security context, PRC network and cyber operations are an integral part of intelligence gathering, just as they are for most other nations, including the United States. Undertaking such efforts is an essential part of the PLA's broader efforts to establish "information dominance," which PLA analysts view as an essential prerequisite to fighting and winning future conflicts. Because of the need to be able to rapidly exploit information more effectively than an adversary in wartime, it is necessary to undertake cyber and electronic reconnaissance of adversaries in peacetime. This includes not only amassing electronic signatures of enemy communications and weapons systems, but also surveying their networks, understanding their organization, and constructing the ability to attack those systems and defend against counter-attacks.

To this end, the Chinese People's Liberation Army (PLA) created a new service, the PLA Strategic Support Force (PLASSF), in the massive restructuring and reorganization announced on December 31, 2015. The PLASSF brings together China's electronic warfare (EW), network and cyber warfare, and space warfare forces into a single entity.[3] As all of these elements are linked to the gathering, exploitation, and transmission of information, the PLASSF is very much China's "information warfare force."

Of special importance here is the Network Systems Department (NSD) of the PLASSF. This component of the PLASSF incorporates element of what had previously been part of the PLA General Staff Department's 3rd Department, which had been responsible for a variety of cyber

[3] For a more extensive discussion of the PLA SSF, please see John Costello and Joe McReynolds, ***China's Strategic Support Force: A Force for a New Era***, INSS China Strategic Perspectives #13 (Washington, DC: National Defense University, October 2018).

espionage activities. This includes the infamous Unit 61398, named in a 2013 Mandiant report and the first PLA unit publicly identified as a hacker force.[4]

The existence of Unit 61398 as a PLA unit also highlights a fundamental difference between Chinese and Western execution of cyber *economic* espionage. There are few reports of Western intelligence or military forces being tasked with economic espionage. By contrast, the PLA is part of a vast network of Chinese cyber forces that undertake economic as well as national security espionage. Five members of Unit 61398, for example, were indicted by the US Department of Justice for various cyber economic espionage activities over the period 2006-2014, including attacks on Alcoa, Allegheny Technologies Inc., and Westinghouse.[5]

As the Office of the Director of National Intelligence noted in their 2023 threat assessment, "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."[6] Similarly, FBI Director Christopher Wray observed in 2020 that Chinese espionage efforts are

> not just targeting defense sector companies. The Chinese have targeted companies producing everything from proprietary rice and corn seeds to software for wind turbines to high-end medical devices. And they're not just targeting innovation and R&D. They're going after cost and pricing information, internal strategy documents, bulk PII—anything that can give them a competitive advantage.[7]

[4] Mandiant, ***APT1: Exposing One of China's Cyber Espionage Units*** (February 2013) https://nsarchive.gwu.edu/document/21484-document-83

[5] Department of Justice Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," (May 19, 2014) https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[6] Office of the Director of National Intelligence, ***Annual Threat Assessment of the US Intelligence Community 2023*** (Washington, DC: ODNI, February 2023), p. 10, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

[7] Christopher Wray, "Responding Effectively to the Chinese Economic Espionage Threat," Remarks at the Department of Justice China Initiative Conference, Center for Strategic and International Studies (February 6, 2020) https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

These efforts in turn incorporate both military and civilian, governmental and non-governmental elements, such that they outnumber the FBI's cyber staff by 50 to 1.[8]

Targeting the U.S. Department of the Interior for Network Attacks

Given the roles and responsibilities of the United States Department of the Interior (DOI), at least some of this massive array of cyber and network attackers are likely targeted at the DOI. For example, the DOI has oversight of US public lands, including drilling and mining rights. Within this purview is oversight of development of leasable minerals, such as oil, natural gas, coal, phosphate, potassium, and sodium, as well as locatable (or hardrock) minerals, such as gold, silver, copper, and gemstones.[9] Such resources are clearly of economic importance.

As important, the United States government has identified an array of 35 critical minerals vital to national economic security, including cobalt, fluorspar, and niobium.[10] Until recently, there have been no surveys of public lands to determine how much, if any, of these critical minerals might be present. Under President Biden's Executive Order 14017, however, the DOI is encouraged to have the US Geological Survey, along with the Bureau of Land Management and the Department of Agriculture's US Forest Service, begin such surveys. For the PRC, accessing the results would provide useful insight into American reserves and potential production capacity for these critical minerals.

Similarly, the DOI has oversight over leasing of both onshore and offshore sites for oil drilling. Knowing the location of potential new energy reserves, including offshore sites, would be strategically valuable, as it could help the Chinese determine which companies, in turn, to monitor and even penetrate through cyber and other means. As important, sites that are tapped will require

---

[8] Lauren Feiner, "Chinese Hackers Outnumber FBI Cyber Staff by 50 to 1, Bureau Director Says," CNBC (April 28, 2023) https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html

[9] Congressional Research Service, ***Federal Lands and Related Resources: Overview and Selected Issues for the 118th Congress***, CRS Report R43429 (February 24, 2023) https://crsreports.congress.gov/product/pdf/R/R43429/42

[10] US Geological Survey Communications and Publishing, "US Geological Survey Releases 2022 List of Critical Minerals," (February 22, 2022) https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals

the construction of substantial networks of pipelines and other infrastructure to extract and move those resources. As a 2021 Joint Cybersecurity Advisory, coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), noted, state-sponsored Chinese actors have repeatedly targeted U.S. oil and natural gas (ONG) pipeline companies in the past.[11]

ONG companies may have their operating software attacked. Alternatively, as with the May 2021 Colonial Pipeline incident, the companies may be targeted for ransomware attacks, where the data is made inaccessible (but is not destroyed). Although Colonial Pipeline's networks moved oil from refineries to customers, other parts of the overall energy supply chain, including from fields to refineries, could also be targeted.[12]

Finally, as the DOI is part of the overall US government bureaucracy, it offers potential access to a range of systems not necessarily related to its purview. The DOI, for example, housed the data center for the Office of Personnel Management (OPM). This was the center that was accessed when OPM was hacked in 2015, exposing the records of some 4 million current and former federal employees. Notably, hearings into the hack indicated that DOI had some 3000 "critical and high risk vulnerabilities."[13]

Oversight of Pacific Island States

Another reason for concern about Chinese network attacks and cyber intrusions into the Department of the Interior is that the Department is responsible for overseeing US relations with several of the microstates of the central Pacific. One example is the Republic of the Marshall Islands (RMI), an independent nation tied to the United States by a Compact of Free Association. It comprises 5 islands and 29 atolls, with a population of some 58,000 people. While only possessing some 70 square miles of dry land, these islands and atolls are spread across 750,000

[11] "Chinese Gas Pipeline Intrusion Campaign, 2011-2013" (July 21, 2021) https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a

[12] "About Shell Pipeline," https://www.shell.us/business-customers/shell-pipeline/about-shell-pipeline.html

[13] "Thousands of Cybersecurity Vulnerabilities Uncovered at Interior Department," FedScoop (July 15, 2015) https://fedscoop.com/after-opm-hack-interior-cybersecurity-audit-finds-thousands-of-critical-vulnerabilities/

square miles of central Pacific territory.[14] As such, they straddle waters that link the American west coast with the east Asian littoral.

This strategic position was made clear during the Second World War, when U.S. forces "island hopped" through the Marshall islands, on their way to the Marianas and eventually to Japan. Indeed, the battles for Kwajalein and Eniwetok provided invaluable experience for later battles on Guam, Iwo Jima, and Okinawa.

In the wake of the Second World War, the United States was granted trusteeship over various central Pacific territories, including the Marshall Islands. The Republic of the Marshall Islands (RMI) gained its independence in 1986. Under the original and subsequently amended Compact of Free Association (CFA), RMI citizens can work, live, and study in the United States, as non-immigrants.[15] As of 2019, there were some 27,000 Marshallese in the United States, a substantial portion of the RMI population.[16]

In addition, under the terms of the CFA, the United States provides RMI with economic support and aid. The United States provides RMI with some $70 million annually in various forms. This includes a jointly managed trust fund. US government agencies and offices, such as the Federal Communications Commission and US Postal Service, also provide services to the Marshall Islands. This aid is scheduled to end when the current amended Compact expires in 2023.

In exchange, the United States is granted exclusive and full authority to RMI lands and waterways for security and defense purposes, although RMI is free to conduct its own foreign relations. A key element of both economic and security ties is the leasing of land and lagoon space to the U.S.

[14] U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Marshall Islands," (July 15, 2018) https://www.state.gov/u-s-relations-with-marshall-islands/

[15] U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Marshall Islands," (July 15, 2018) https://www.state.gov/u-s-relations-with-marshall-islands/

[16] Susanne Rust, "They Came Here After the U.S. Irradiated Their Islands. Now They Face an Uncertain Future," ***Los Angeles Times*** (December 31, 2019) https://www.latimes.com/world-nation/story/2019-12-31/marshall-islands-uncertain-future-us-marshallese-spokane

Army on Kwajalein atoll under the Military Use and Operating Rights Agreement. The missile and space facilities there are the second largest employer in the RMI.[17]

RMI's Role in American Defense Efforts

Throughout the post-war period, the Marshall Islands have played an important role in America's defense, especially in the context of nuclear deterrence.

In the immediate post-war period, the United States conducted an array of nuclear tests in the Marshall Islands. The 67 nuclear tests conducted there between 1946 and 1958 included Castle Bravo, the largest American nuclear test involving a 15 megaton device.[18] It is worth noting that this test was nonetheless dwarfed by four Soviet tests, which ranged from 20-50 megatons.

With the Limited Test Ban Treaty of 1963, which effectively banned above-ground nuclear tests, the islands have no longer been rocked by nuclear explosions. RMI has continued to play an important role, however, in maintaining America's nuclear deterrent posture. Especially important has been the role of Kwajalein and the Ronald Reagan Ballistic Missile Defense Test Site (RTS).

The RTS provides key support to US defense efforts in several ways. The credibility of the American nuclear deterrent is sustained through a program of regular tests of Minuteman III missiles. As recently as August of 2021, the US fired a Minuteman III with a Hi Fidelity Joint Test Assembly re-entry vehicle onboard towards Kwajalein.[19] Such tests demonstrate to all observers, including America's adversaries, the continuing functionality and reliability of the American nuclear deterrent. This is becoming an ever more pressing issue due to the aging of the Minuteman III, first introduced in the 1960s.

[17] U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Marshall Islands," (July 15, 2018) https://www.state.gov/u-s-relations-with-marshall-islands/

[18] Lawrence Livermore National Laboratories, "Brief History of Nuclear Testing in the Marshall Islands," (July 28, 2021) https://marshallislands.llnl.gov/testhistory.php

[19] Air Force Global Strike Command Public Affairs, "Minuteman III Test Launch Showcases Readiness of U.S. Nuclear Forces' Safe, Effective Deterrent," (August 11, 2021) https://www.stratcom.mil/Media/News/News-Article-View/Article/2727368/minuteman-iii-test-launch-showcases-readiness-of-us-nuclear-forces-safe-effecti/

The fact that these test shots cover some 4200 miles further enhances the credibility of the American deterrent. Russian ICBM tests from the Plesetsk Kosmodrome to the Kura test range in Kamchatka cover some 3800 miles.[20] Longer test flights provide more opportunity for measurements of flight characteristics.

Moreover, given the size of the Kwajalein lagoon (which is one of the largest in the world at over 600 square miles), one can target warheads and dummy payloads into it, and thereby prevent their recovery by other actors. In 2016, Chinese sailors seized an American unmanned underwater vehicle (UUV) from international waters.[21] There should be little doubt that the Chinese, among others, would very much like an opportunity to examine a dummy US nuclear warhead.

The facilities at Kwajalein also support missile defense efforts. The various radars and facilities provide American missile defense planners and engineers with data to help improve missile interception capability. This is of growing concern, as both Russia and China modernize their own nuclear arsenals.

Nor are missile defenses only relevant to the nuclear side of the deterrence equation. The PRC, for example, has deployed anti-ship ballistic missiles, such as the DF-21 and DF-26. Both of these are clearly intended to neutralize American aircraft carriers and other maritime strategic platforms. Missile defenses would degrade Chinese confidence that they can sink or damage American carriers, which in turn would help deter China from using force against various neighbors, from Japan to Taiwan to the Philippines.

In November 2020, an American SM-3 Block IIA missile successfully intercepted an ICBM-type missile, launched from Kwajalein.[22] This was the first time that the SM-3, which can be deployed

[20] Joe Saballa, "Russia to Test Launch Advanced intercontinental Ballistic Missile," ***Defense Post*** (May 5, 2021) https://www.thedefensepost.com/2021/05/05/russia-to-test-launch-ballistic-missile/

[21] Terri Moon Cronk, "Chinese Seize U.S. Navy Underwater Drone in South China Sea," ***DOD News*** (December 16, 2016) https://www.defense.gov/News/News-Stories/Article/Article/1032823/chinese-seize-us-navy-underwater-drone-in-south-china-sea/

[22] The Department of Defense, "U.S. Successfully Conducts SM-3 Block IIA Intercept Test Against an Intercontinental Ballistic Missile Target," (November 17, 2020) https://www.defense.gov/News/Releases/Release/Article/2417334/us-successfully-conducts-sm-3-block-iia-intercept-test-against-an-intercontinen/

aboard an AEGIS-equipped destroyer or cruiser, had destroyed such a target.[23] This radically improves not only American deterrence, but that of any allied nation that has comparable AEGIS-type systems in their fleet. The SM-3 is already part of the Phased Adaptive Approach for NATO defense against Russian missile threats. It is deployed in the ground-based site in Rumania, and will be deployed to the site currently under construction in Poland. Meanwhile, Japan has chosen to rely on its fleet of AEGIS destroyers to provide missile defense for the Home Islands, against North Korean and Chinese threats. The success of the SM-3 Block IIA test means that this key US ally will be more secure in coming years. The facilities in the Marshall Islands have played a key role in improving American and allied security.

Finally, the facilities in the RMI, including on Kwajalein, play a central role in space surveillance. The United States Space Force currently tracks some 26,000 objects in space. Because of the high speed of objects in orbit, even a bolt or a screw can do enormous damage to the International Space Station or an orbiting satellite. The recently built Space Fence on Kwajalein provides the Space Force with the ability to monitor objects as small as a marble.[24]

This capability is of growing importance as America's competitors and adversaries develop ever more capable space systems, many of which are believed to be anti-satellite systems. The Russians, for example, have deployed sub-satellites from larger satellites, much like submunitions from a dispenser. In 2017, Kosmos-2519 launched Kosmos-2521, a sub-satellite while in orbit. Kosmos-2521 subsequently launched a sub-satellite of its own, Kosmos-2523. Both Kosmos-2519 and Kosmos-2521 maneuvered in orbit.[25] Meanwhile, China's new reusable space plane apparently released an object while in orbit, and engaged in rendezvous and proximity operations (RPO) with at least one other object over the past year.[26] All of these actions are difficult to track, especially

---

[23] The War Zone Staff, "The Navy Has Finally Proven It Can Shoot Down an Intercontinental Ballistic Missile***," The Drive*** (November 17, 2020) https://www.thedrive.com/the-war-zone/37685/the-navy-has-finally-proven-it-can-shoot-down-an-intercontinental-ballistic-missile

[24] Sandra Erwin, "Space Fence Surveillance Radar Site Declared Operational," ***Space News*** (March 28, 2020) https://spacenews.com/space-fence-surveillance-radar-site-declared-operational/

[25] Gunter D. Krebs, "Kosmos-2519/Kosmos-2521/Kosmos-2523," ***Gunter's Space Page*** Retrieved October 17, 2021, https://space.skyrocket.de/doc_sdat/kosmos-2519.htm

[26] Andrew Jones, "China's Mysterious Spaceplane Releases Object into Orbit," ***Space News*** (November 2, 2022) https://spacenews.com/chinas-mystery-spaceplane-releases-object-into-orbit/, and Joseph Trevithick, "Chinese Spaceplane Docked with Another Object Multiple Times Data Indicates," ***The Drive*** (May 9, 2023)

while also maintaining situational awareness over 26,000 pieces of other debris. Russia has since launched other satellites that have behaved in a similar fashion, launching their own sub-satellites.[27] US space surveillance capabilities must maintain watch over all these objects, if America's own satellites are to be preserved.

The ground-based Space Fence radar on Kwajalein is an essential part of the American space surveillance network. It plays a key role in helping the U.S. detect and track potential threats to its satellites, including its missile early warning, strategic communications, and reconnaissance platforms.

In addition to RMI, the United States has comparable special relationships with the Federated States of Micronesia, and the Republic of Palau. Relations with both of these states are also overseen by the DOI. Both of these states are slated for additional US military construction, but have also been courted by Beijing.[28]

For the PRC, which has been seeking inroads into the central Pacific and to build expanded ties to the various states, gaining insider knowledge of American positions, aid packages, and general policy towards those states would be of enormous strategic advantage. Moreover, as both RMI and the Republic of Palau maintain ties with Taiwan, rather than the PRC, Beijing is intensely interested in gaining any leverage it can to shift their diplomatic alignment.

https://www.thedrive.com/the-war-zone/chinese-spaceplane-docked-with-another-object-multiple-times-data-indicates

[27] Neel V. Patel, "The U.S. Says Russia Just Tested an 'Anti-Satellite Weapon' in Orbit," ***Technology Review*** (July 23, 2020) https://www.technologyreview.com/2020/07/23/1005568/us-space-command-russia-test-anti-satellite-weapon-orbit-kosmos-2543/

[28] Kirsty Needham, "Pacific Islands a Key U.S. Military Buffer to China's Ambitions, Report Says," Reuters (September 20, 2022) https://www.reuters.com/world/asia-pacific/pacific-islands-key-us-military-buffer-chinas-ambitions-report-2022-09-20/